Amendment

Not withstanding the foregoing, to help expedite and streamline the prosecution, Applicants hereby amend the pending claims as follows:

1. (Original) A system of secure network connectivity between one or more users and at least one network server, comprising:

at least one intelligent data carrier, issued to one user, wherein said intelligent data carrier comprises at least (i) one memory, adapted to store data, (ii) one input-output apparatus, adapted to input and output data, and (iii) one processor, adapted to process the data stored in said memory, wherein said intelligent data carrier is capable of connecting to a host computer device thereby transmitting data via said input-output apparatus over the network, and wherein said intelligent data carrier is adapted to establish a network identity for the user through an authentication and encryption scheme; and

a dynamic datagram switch for dynamic allocation and swapping of datagrams for a multiplicity of applications in service to the one or more users.

2. (Original) The system of claim 1, wherein said intelligent data carrier is mobile.

3. (Original) The system of claim 1, wherein said intelligent data carrier is implemented with one of USB key, Compact Flash, Smart Media, Compact Disk, DVD, PDA, firewire device, and token device.

4-22 (Cancelled)

23. (Currently amended) The system of claim 1, wherein said multiplicity of applications comprises at least one of window-based remote terminal server applications, applications on 3270/5250 terminal emulators for mainframe, directly embedded applications, and multimedia applications, wherein the directly embedded applications comprise at least one of database applications, data analysis tools, Customer Relation Management [[(CRM)]] tools, and Enterprise Resource Planning [[(ERP)]] packages.

24. (Currently amended) The system of claim 1, wherein said dynamic datagram switch comprises a datagram schema and a parser, wherein said datagram schema comprises two or more datagrams, belonging to one or more datagram types, ~~wherein said datagram is adapted to carry (i) content data for network transmission and (ii) other information for managing and controlling network connects and support network applications,~~ wherein each datagram type comprises a plurality of functions, and wherein said parser is adapted to parse the one or more datagram types.

25. (Original) The system of claim 24, wherein said datagram schema comprises at least one major datagram type and within said one major datagram type, at least one minor datagram type.

26. (Original) The system of claim 25, wherein the parser is adapted to parse a matrix of datagram types, said matrix comprising a first multiplicity of major datagram types and in each major datagram type of said first multiplicity, a second multiplicity of minor datagram types.

27. (Currently amended) The system of claim 26, wherein the major datagram type is selected from the group consisting of (i) a[[the]] server messages and connection control datagram, adapted to authenticate and control user connections, (ii) a[[the]] content datagram, adapted to transmit the content data, (iii) a[[the]] broadcast datagram, adapted to manage point-to-point, point-to-multipoint, and multipoint-to-multipoint data transmission, (iv) a[[the]] connection proxy datagram, adapted to pass proxy data between the network server and the intelligent data carrier, (v) a[[the]] instant message type, adapted to transmit messages in real-time, (vi) a[[the]] large content transfer datagram, adapted to transfer oversized data and media files, (vii) a[[the]] user directory datagram, adapted to search for network users, and (viii) a[[the]] remote management datagram, adapted to remotely control network users.

28. (Currently amended) The system of claim 27, wherein the server messages and connection control datagram comprises ~~at least one of~~ minor datagram types selected from the group consisting of: (i) a[[the]] authentication request datagram, adapted to initiate an authentication request, (ii) a[[the]] authentication reply datagram, adapted to send a response upon a request of authentication, and (iii) a[[the]] authentication result datagram, adapted to send the result of an authentication session.

29. (Currently amended) The system of claim 28, wherein the content datagram comprises ~~at least one of~~ minor datagram types selected from the group consisting of: (i) a[[the]] normal content datagram, adapted to transmit the content data, (ii) a[[the]] remote logging datagram, adapted to communicate with the network server and establish a login session, ~~and~~ (iii) a[[the]] remote data collector datagram, adapted to transmit data from a remote connection,[[.]] (iv) a[[the]] content approval request datagram, adapted to request verification of the content data transmitted, and (v) a[[the]] content approval reply datagram, adapted to respond to a request of verification of the content data transmitted.

30. (Cancelled)

31. (Currently amended) The system of claim 27, wherein the connection proxy datagram comprises ~~at least one of~~ minor datagram types selected from the group consisting of: (i) proxy data to server, adapted to pass proxy data to the network server from the intelligent data carrier, and (ii) proxy data from server, adapted to pass the proxy data from the network server to the intelligent data carrier.

32. (Currently amended) The system of claim 27, wherein the instant message type comprises ~~at least one of~~ minor datagram types selected from the group consisting of: (i) a[[the]] file transmission type, (ii) a[[the]] audio-video transmission type, (iii) a[[the]] instant mail message type, and (iv) a[[the]] remote data collection type.

33. (Currently amended) The system of claim 1[[24]], wherein each datagram in the datagram schema has a generic layout comprising:

(A) header fields for (i) one or more major datagram types, (ii) one or more minor datagram type, (ii) the datagram length, and (iii) a datagram checksum, and

(B) a datagram payload for carrying data in transmission.

34. (Original) The system of claim 33, wherein the generic layout comprises one or more additional header fields.

35. (Original) The system of claim 33, wherein the generic layout follows a TCP header.

36. (Original) The system of claim 1, wherein the intelligent data carrier further comprises a radar connector, wherein the radar connector interfaces the network and is adapted to monitor and control network connections.

37. (Original) The system of claim 36, wherein the network server further comprises a radar connector adapted to monitor and control network connections, wherein the radar connector of the network server is connected to the radar connector of the intelligent data carrier over the network.

38. (Original) The system of claim 37, wherein said radar connector is further adapted to detect lost connections and initialize contact to the network server thereby reestablishing connections.

39. (Original) The system of claim 1, further comprising an injector, adapted to connect an existing networks to the network server and transmit data between said existing network and the intelligent data carrier via the network server, wherein said existing network is wired or wireless.

40. (Original) The system of claim 39, wherein the injector further comprises a radar connector, interfacing the network and adapted to monitor and control network connections.

41. (Original) A client-server communication system, comprising:

at least one server, comprising a dynamic datagram switch for dynamic allocation and swapping of datagrams for a multiplicity of network applications; and

at least one client, wherein the client is an intelligent data carrier, comprising at least (i) one memory, adapted to store data, (ii) one input-output apparatus, adapted to input and output data, and (iii) one processor, adapted to process the data stored in said memory, wherein said intelligent data carrier is capable of connecting to a host computer device thereby transmitting data via said input-output apparatus over the network, and wherein said intelligent data carrier is adapted to establish a network user identity through an authentication and encryption scheme for secure data transmission between said server and said client.

42. (Cancelled)

43. (Currently amended) The client-server communication system of claim [42]41, wherein said intelligent data carrier is implemented with one of USB key, Compact Flash, Smart Media, Compact Disk, DVD, PDA, firewire device, and token device.

44. (Currently amended) The client-server communication system of claim 41, wherein said dynamic datagram switch comprises a datagram schema and a parser, wherein said datagram schema comprises two or more datagrams, belonging to one or more datagram types, ~~wherein said datagram is adapted to carry (i) content data for network transmission and (ii) other information for managing and controlling network connects and support network applications,~~ wherein each datagram type comprises a plurality of functions, and wherein said parser is adapted to parse the one or more datagram types.

45. (Currently amended) The client-server communication system of claim 41[[44]], wherein said datagram schema comprises at least one major datagram type and within said one major datagram type, at least one minor datagram type.

46. (Currently amended) The client-server communication system of claim 41[[44]], wherein the parser is adapted to parse a matrix of datagram types, said matrix comprising a first multiplicity of major datagram types and in each major datagram type of said first multiplicity, a second multiplicity of minor datagram types.

47. (Currently amended) The client-server communication system of claim 41[[46]], wherein each datagram in the datagram schema has a generic layout comprising:

(A) header fields for (i) one or more major datagram types, (ii) one or more minor datagram type, (ii) the datagram length, and (iii) a datagram checksum, and

(B) a datagram payload for carrying data in transmission.

48-66. (Cancelled)

67. (Original) The client-server communication system of claim 41, further comprising an injector, adapted to connect an existing network to the server and transmit data between the existing networks and the client via the server, wherein the existing network is wired or wireless.

68. (Original) The client-server communication system of claim 67, wherein the server, client, and injector each comprises a radar connector, wherein the radar connector interfaces the network and is adapted to monitor and control network connections, wherein the radar connector of the client is connected to the radar connector of the server over the network, and wherein the radar connector of the injector is connected to the radar connector of the server over the network.

69. (Original) The client-server communication system of claim 68, wherein the radar connector of the client is further adapted to detect lost connections and initialize contact to the server thereby reestablishing connections.

70. (Original) The client-server communication system of claim 41, wherein the server further comprises an encrypted virtual file system for dedicated data storage for the client.

71. (Currently amended) An intelligent data carrier, comprising at least (i) one memory, adapted to store data, (ii) one input-output apparatus, adapted to input and output data, and (iii) one processor, adapted to process the data stored in said memory, wherein the intelligent data carrier is capable of connecting to a host computer device on a network thereby transmitting data via said input-output apparatus over the network, wherein the data transmission is through dynamically-switched datagrams in a datagram schema, wherein the intelligent data carrier is adapted to establish a network user identity through an authentication and encryption scheme for secure network data transmission.

72-91. (Cancelled)

92. (Currently amended) The intelligent data carrier of claim 71[[91]], said intelligent data carrier is implemented with one of USB keys, Compact Flash, Smart Media, Compact Disks, DVDs, PDAs, firewire devices, and token devices.

93. (Original) The intelligent data carrier of claim 71, wherein the dynamically-switched datagrams belong to one or more datagram types and are adapted to carry (i)

content data for network transmission and (ii) other information for managing and controlling network connections and supporting network applications, wherein each datagram type comprises a plurality of functions.

94. (Original) The intelligent data carrier of claim 93, wherein the datagram types comprise at least one major datagram type and within the major datagram type, at least one minor datagram type.

95. (Original) The intelligent data carrier of claim 94, wherein the datagrams conform to a generic layout, said generic layout comprising:

(A) header fields for (i) one or more major datagram types, (ii) one or more minor datagram type, (ii) the datagram length, and (iii) a datagram checksum, and

(B) a datagram payload for carrying data in transmission.

96. (Original) A method for secure network communication, comprising:

issuing to a network user an intelligent data carrier, wherein the intelligent data carrier comprises at least (i) one memory, adapted to store data, (ii) one input-output apparatus, adapted to input and output data, and (iii) one processor, adapted to process the data stored in said memory, wherein the intelligent data carrier is capable of connecting to a host computer device on the network thereby transmitting data via said input-output apparatus over the network, wherein the intelligent data carrier is adapted to establish a network identity for the network user through an authentication and encryption scheme; and

providing a dynamic datagram switch in a server on the network for dynamic allocation and swapping of datagrams in support of a multiplicity of applications.

97-98. (Cancelled)

99. (Currently amended) The method of claim 96, wherein said dynamic datagram switch comprises a datagram schema and a parser, wherein said datagram schema comprises two or more datagrams, belonging to one or more datagram types, ~~wherein said datagram is adapted to carry (i) content data for network transmission and (ii) other information for managing and controlling network connects and support network applications,~~ wherein each datagram type comprises a plurality of functions, and wherein said parser is adapted to parse the one or more datagram types.

100-102.(Cancelled)

103. (Currently amended) The method of claim 96, wherein the authentication and encryption scheme comprises the following sequential steps:

(a) a request being caused to forward from the intelligent data carrier to the server that the intelligent data carrier be authenticated;

(b) the server presenting to the intelligent data carrier a plurality of authentication methods;

(c) the intelligent data carrier selecting one authentication method from said plurality through an event;

(d) the server sending the intelligent data carrier a demand, based on said selected method, for authentication data from the intelligent data carrier;

(e) the server transforming said authentication data received from the intelligent data carrier into one or more data authentication objects, wherein each of said data authentication objects [[object]] is a data vector object, capable of being analyzed using one or more classifiers;

(f) the server analyzing said data authentication objects, according to said one or more classifiers, thereby determining the result of the authentication; and

(g) the server sending said result to the intelligent data carrier, indicating a successful or failed authentication attempt.

104. (Original) The method of claim 103, wherein said event in step (c) comprises at least one of a click of a mouse, a touch on a screen, a keystroke, an utterance, and a biometric measurement.

105. (Currently amended) The method of claim 103, wherein said demand in step (d) comprises at least one of a pseudo random and a true random code, wherein the[[a]] pseudo random code is generated based on a mathematically pre-calculated list, and wherein the[[a]] true random code is generated by sampling and processing a source of entropy outside of the system.

106. (Cancelled)

107. (Currently amended) The method of claim 103, wherein said analyzing in step (f) is performed based on one or more analysis rules, wherein said one or more analysis rules comprise classification according to the one or more classifiers of step (e).

108. (Cancelled)

109. (Currently amended) The method of claim 107[[108]], wherein said classification comprises speaker verification, wherein the data object vectors involve two classes, the target speaker and the impostor, wherein each class is characterized by a probability density function, and wherein the determining in step (f) is a binary decision problem.

110. (Currently amended) The method of claim 103, wherein said determining in step (f) comprises computing at least one of the sum, superiority, and probability from said one or more data vector objects, based on the one or more classifiers of step (e), wherein the sum is one of a superior and a random sum computed from the one or more data vector objects.

111. (Cancelled)

112. (Currently amended) The method of claim 103, wherein said one or more classifiers in step (e) comprise a super classifier derived from the more than one data vector objects, wherein said super classifier is based on one of physical biometrics and performance biometrics, wherein physical biometrics comprises at least one of voice recognition, fingerprints, handprints, blood vessel patterns, DNA tests, retinal or iris scan, and face recognition, wherein performance biometrics comprises habits or patterns of individual behaviors.

113-114. (Cancelled)

115. (Currently amended) The method of claim 96, wherein said authentication and encryption scheme comprises symmetrical and asymmetrical multi-cipher encryption, wherein said encryption uses at least one of output feedback, cipher feedback, cipher forwarding, and cipher block chaining.

116. (Cancelled)

117. (Currently amended) The method of claim 115[[116]], wherein the encryption is based on Advanced Encryption Standard (AES) Rijndael.

118. (Currently amended) The method of claim 96, wherein said authentication and encryption scheme implements Secure Key Exchange [[(SKE)]], wherein the Secure Key Exchange employs one of a public key system and Elliptic Curve Cryptosystem private keys.

119-120. (Cancelled)

121. (Original) The method of claim 96, wherein the authentication and encryption scheme comprises at least one of a logic test adapted to validate that the intelligent data carrier has been registered with the server, a device test adapted to validate the physical parameters at the intelligent data carrier and the host computer device, and a personal test adapted to authenticate the user based on event-level data.

122. (Original) The method of claim 96, further comprising providing a first radar connector in the intelligent data carrier and a second radar connector in the server, wherein the first radar connector is adapted to connected to the second radar connector over the

network, wherein the first and the second radar connector are adapted to monitor and control network connections.

123. (Original) The method of claim 122, wherein the first radar connector is further adapted to detect lost connections and initialize contact to the second radar connector thereby reestablishing connections.

124. (Original) The method of claim 96, further comprising providing an encrypted virtual file system in the server for dedicated data storage for the client.

125. (Original) The method of claim 96, wherein the dynamic datagram switch performs datagram allocation and swapping in real time.

126. (Original) The method of claim 96, wherein the dynamic datagram switch performs datagram allocation and swapping based on memory pointers of two or more datagrams.

127. (Currently amended) A method for target delivery of one or more applications to a user, comprising:

issuing the user an intelligent data carrier, adapted to dock onto a host computer device that is connected to a network on which a network server sits and communicate with the network server over the network, wherein the network server communicates with the intelligent data carrier through dynamically-switched datagrams in a datagram schema, wherein the intelligent data carrier comprises at least (i) one memory, adapted to store data, (ii) one input-output apparatus, adapted to input and output data, and (iii) one processor, adapted to process the data stored in said memory;

the server authenticating the user through an authentication and encryption scheme; and

granting the user access to the one or more applications upon successful authentication.

128. (Original) The method of claim 127, wherein said one or more applications are preloaded on the intelligent data carrier or installed on the network server or the host computer device.

129. (Original) The method of claim 128, wherein the host computer device is connected to the network via wired or wireless means.

130. (Original) The method of claim 128, wherein the host computer device comprises at least one of a desktop or laptop computer, a personal digital assistant (PDA), a mobile phone, a digital TV, an audio or video player, a computer game consol, a digital camera, a camera phone, and a network-enabled domestic appliance.

131. (Original) The method of claim 130, wherein the network-enabled domestic appliance is one of a network-enabled refrigerator, microwave, washer, dryer, and dishwasher.

132. (Currently amended) The method of claim 127, wherein said one or more applications comprise at least one of window-based remote terminal server applications, applications on 3270/5250 terminal emulators for mainframe, directly embedded applications, and multimedia applications, wherein the directly embedded applications comprise at least one of database applications, data analysis tools, Customer Relation Management [[(CRM)]] tools, and Enterprise Resource Planning [[(ERP)]] packages.

133-160. (Cancelled)